IN THE TITLE:

Please add the following to the title on record

--UTILIZING A KEY FOR ENCIPHERING AND DECIPHERING THAT IS

MODIFIED DURING ENCIPHERING AND DECIPHERING--.

IN THE SPECIFICATION:

Page 18, line 4, please change "has(ID...)" to

--hash(ID...)--.

Page 31, line 6, please change "applying LK' stored" to --

applying LK stored--.

IN THE CLAIMS:

Please cancel claims 14 and 15.

Applicants have requested amendment to claims 1, 3-5, 9-11,

13 and 16-17, a copy of each of these claims being presented

herein. A marked-up version of these claims indicating

insertions and deletions is included as an attachment to this

amendment.

1.   (Amended)   An enciphering apparatus for enciphering data

using a cryptographic key, comprising:

first providing means for providing a first information

which is changed during a predetermined session;

second providing means for providing a second information

which is changed during the predetermined session;

producing means for producing a cryptographic key based on

the first information which is changed during the predetermined

session and the second information which is changed during the predetermined session; and

a1

enciphering means or enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

3. (Amended) An enciphering apparatus according to claim 1, wherein said producing means produces said cryptographic key with which a correct decipherment result is obtained even if the first information and the second information which are used to generate said cryptographic key are used individually to successively decipher the enciphered data.

4. (Amended) An enciphering apparatus according to claim 1, wherein said producing means adds the second information to a value whose initial value is the first information to produce the cryptographic key.

5. (Amended) An enciphering apparatus according to claim 4, wherein the first information has a number of bits larger than that of the second information, and said producing means adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

9. (Amended) An enciphering method for enciphering data using a cryptographic key, comprising the steps of:

providing a first information which is changed during a predetermined session;

providing a second information which is changed during the predetermined session;

producing a cryptographic key based upon the first information which is changed during said predetermined session and the second information which is changed during the predetermined session; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

10. (Amended) A deciphering apparatus for deciphering data using a cryptographic key, comprising:

receiving means for receiving enciphered data;

first providing means for providing a first information which is changed during a predetermined session;

second providing means for providing a second information which is changed during the predetermined session;

producing means for producing a cryptographic key based upon the first information which is changed during the predetermined session and the second information which is changed during the predetermined session; and

deciphering means for deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key

is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

11. (Amended) A deciphering apparatus according to claim 10, wherein said producing means includes first producing means for producing a first cryptographic key based upon one of the first information and the second information, and second producing means for producing a second cryptographic key based upon the other of the first information and the second information, and said deciphering means includes first deciphering means for deciphering the enciphered data based upon the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further based upon the second cryptographic key.

13. (Amended) A deciphering method for deciphering data using a cryptographic key, comprising the steps of:

receiving enciphered data;

providing a first information which is changed during a predetermined session;

providing a second information which is changed during the predetermined session;

producing a cryptographic key based upon the first information which is changed during the predetermined session and the second information which is changed during the predetermined session; and

deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

16. (Amended) An information processing apparatus, comprising:

receiving means for receiving enciphered data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second cryptographic key based upon a first information which is changed during a predetermined session and a second information which is changed during the predetermined session;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second cryptographic key produced by said producing means, wherein said second cryptographic key is changed while said data is being deciphered.

17. (Amended) An information processing method, comprising the steps of:

receiving enciphered data transmitted thereto through a bus;

Page 6

producing, from the received data, a first cryptographic key, and a second cryptographic key based upon a first information which is changed during a predetermined session and a second information which is changed during the predetermined session;

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second cryptographic key, wherein said second cryptographic key is changed while said data is being deciphered.

Please add new claims 18-72 as follows:

18. An enciphering apparatus for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon a first information provided by said first information provider and which is changed during a predetermined session, and a second information provided by said second information provider and which is changed during the predetermined session, said second

information being changed at a predetermined time while the data is being enciphered.

19. The enciphering apparatus according to claim 18, wherein said cryptographic key producer produces a homomorphic cryptographic key.

20. The enciphering apparatus according to claim 18, wherein said cryptographic key producer produces said cryptographic key with which a correct decipherment result is obtained even if a first information and a second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

21. The enciphering apparatus according to claim 18, wherein said cryptographic key producer adds the second information to a value whose initial value is the first information to produce the cryptographic key.

22. The enciphering apparatus according to claim 21, wherein the first information has a number of bits larger than that of the second information, and said cryptographic key producer adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

23. The enciphering apparatus according to claim 22, wherein said cryptographic key producer further updates the

result of the addition with the further addition of the extracted bit.

24. The enciphering apparatus according to claim 23, wherein said cryptographic key producer selects predetermined bits from a result of the further addition of the extracted bits at a predetermined timing to produce the cryptographic key.

25. The enciphering apparatus according to claim 18, further comprising a transmitter coupled with said encipherer; said transmitter transmitting the data enciphered with a cryptographic key to another apparatus via a bus.

26. A deciphering apparatus for deciphering data using a cryptographic key, comprising:

a receiver;

a decipherer coupled with said receiver;

a first information provider coupled with said decipherer;

a second information provider coupled with said decipherer; and

a cryptographic key producer coupled with said decipherer, whereby said decipherer deciphers data received by said receiver using a cryptographic key produced by said cryptographic key producer based upon a first information provided by said first information provider and which is changed during a predetermined session and a second information provided by said second information provider which is changed during the predetermined session, said second information being changed at a predetermined

time while the data is being deciphered by said deciphering apparatus.

27. The deciphering apparatus according to claim 26, wherein said cryptographic key producer includes a first cryptographic key producer coupled with said first and second information providers for producing a first cryptographic key using one of the first information and the second information, and a second cryptographic key producer coupled with said first and second information providers and said first cryptographic key producer for producing a second cryptographic key using the other of the first information and the second information, and said decipherer includes a first deciphering section and a second deciphering section, said first deciphering section deciphering the enciphered data using the first cryptographic key, and said second deciphering section deciphering the data deciphered by said first deciphering section using the second cryptographic key.

28. The deciphering apparatus according to claim 27, wherein said second deciphering section is formed from application software for processing the deciphered data.

29. An enciphering method according to claim 9, wherein a homomorphic cryptographic key is produced.

30. An enciphering method according to claim 9, wherein said cryptographic key is produced with which a correct decipherment result is obtained even if the first information and

the second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

31. An enciphering method according to claim 9, wherein the second information is added to a value whose initial value is the first information to produce the cryptographic key.

32. An enciphering method according to claim 31, wherein the first information has a number of bits larger than that of the second information, and the second information is added to bits at predetermined positions of the first information, a bit at a predetermined position of a result of the addition is extracted and the extracted bit is further added to produce the cryptographic key.

33. An enciphering method according to claim 32, wherein the predetermined bits of the result of the addition are updated with a result of the further addition of the extracted bit.

34. An enciphering method according to claim 33, wherein predetermined bits are selected from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

35. An enciphering method according to claim 9, further comprising the step of transmitting the data enciphered with the cryptographic key to another apparatus via a bus.

36. A deciphering method according to claim 13, wherein a first cryptographic key is produced using one of the first information and the second information, and a second

cryptographic key is produced using the other of the first information and the second information, and the enciphered data is first deciphered using the first cryptographic key, the data deciphered using the first cryptographic key is further deciphered using the second cryptographic key.

37. A deciphering apparatus according to claim 36, wherein deciphering using said second cryptographic key is performed by application software for processing the deciphered data.

38. An enciphering apparatus for enciphering data using a cryptographic key, comprising:

first providing means for providing a first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing a second information which is changed while the data is being enciphered;

producing means for producing the cryptographic key based on the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering means or enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

39. An enciphering apparatus according to claim 38, wherein said producing means produces a homomorphic cryptographic key.

40. An enciphering apparatus according to claim 38, wherein said producing means produces said cryptographic key with which a correct decipherment result is obtained even if the first information and the second information which are used to generate said cryptographic key are used individually to successively decipher the enciphered data.

41. An enciphering apparatus according to claim 38, wherein said producing means adds the second information to a value whose initial value is the first information to produce the cryptographic key.

42. An enciphering apparatus according to claim 41, wherein the first information has a number of bits larger than that of the second information, and said producing means adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

43. An enciphering apparatus according to claim 42, wherein said producing means further updates the predetermined bits of the result of the addition with a result of the further addition of the extracted bit.

44. An enciphering apparatus according to claim 43, wherein said producing means selects predetermined bits from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

45.   An enciphering apparatus according to claim 38, further comprising transmission means for transmitting the data enciphered with the cryptographic key to another apparatus via a bus.

46. An enciphering method for enciphering data using a cryptographic key, comprising the steps of:

providing a first information which is held in common with another device in an authentication process by communication between the two devices;

providing a second information which is changed while the data is being enciphered;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

47. A deciphering apparatus for deciphering data using a cryptographic key, comprising:

receiving means for receiving enciphered data;

first providing means for providing a first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing a second information which is changed while the data is being deciphered;

producing means for producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

deciphering means for deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

48. A deciphering apparatus according to claim 47, wherein said producing means includes first producing means for producing a first cryptographic key based upon one of the first information and the second information, and second producing means for producing a second cryptographic key based upon the other of the first information and the second information, and said deciphering means includes first deciphering means for deciphering the enciphered data based upon the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further based upon the second cryptographic key.

49. A deciphering apparatus according to claim 48, wherein said second deciphering means is formed from application software for processing the deciphered data.

50. A deciphering method for deciphering data using a cryptographic key, comprising the steps of:

receiving enciphered data;

providing a first information which is held in common with another device in an authentication process by communication between the two devices;

providing a second information which is changed while the data is being deciphered;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

51. An information processing apparatus, comprising:

receiving means for receiving enciphered data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second cryptographic key based upon a first information which is held in common with another device in an authentication process by communication between the two devices and a second information which is changed while the data is being deciphered;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second cryptographic key produced by said producing means, wherein said second cryptographic key is changed in accordance with said second information while said data is being deciphered.

52. An information processing method, comprising the steps of:

receiving enciphered data transmitted thereto through a bus;

producing, from the received data, a first cryptographic key, and a second cryptographic key based upon a first information held in common with another device in an authentication process by communication between the two devices and a second information which is changed while the data is being deciphered;

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second cryptographic key, wherein said second cryptographic key is changed in accordance with the second information while said data is being deciphered.

53. An enciphering apparatus for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon a first information provided by said first information provider and which is held in common with another device in an authentication process by communication between the two devices, and a second information provided by said second information provider and which is changed while the data is being enciphered, said second information being used for changing the cryptographic key.

54. The enciphering apparatus according to claim 53, wherein said cryptographic key producer produces a homomorphic cryptographic key.

55. The enciphering apparatus according to claim 53, wherein said cryptographic key producer produces said cryptographic key with which a correct decipherment result is obtained even if a first information and a second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

56. The enciphering apparatus according to claim 53, wherein said cryptographic key producer adds the second information to a value whose initial value is the first information to produce the cryptographic key.

57. The enciphering apparatus according to claim 56, wherein the first information has a number of bits larger than that of the second information, and said cryptographic key producer adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

58. The enciphering apparatus according to claim 57, wherein said cryptographic key producer further updates the result of the addition with the further addition of the extracted bit.

59. The enciphering apparatus according to claim 58, wherein said cryptographic key producer selects predetermined bits from a result of the further addition of the extracted bits at a predetermined timing to produce the cryptographic key.

60. The enciphering apparatus according to claim 53, further comprising a transmitter coupled with said encipherer; said transmitter transmitting the data enciphered with a cryptographic key to another apparatus via a bus.

61. A deciphering apparatus for deciphering data using a cryptographic key, comprising:

a receiver;

a decipherer coupled with said receiver;

a first information provider coupled with said decipherer;

a second information provider coupled with said decipherer; and

a cryptographic key producer coupled with said decipherer, whereby said decipherer deciphers data received by said receiver using a cryptographic key produced by said cryptographic key producer based upon a first information provided by said first information provider and which is held in common with another device in an authentication device by communication between the two devices and a second information provided by said second information provider which is changed while the data is being deciphered, said second information being used for changing the cryptographic key.

62. The deciphering apparatus according to claim 61, wherein said cryptographic key producer includes a first cryptographic key producer coupled with said first and second information providers for producing a first cryptographic key using one of the first information and the second information, and a second cryptographic key producer coupled with said first and second information providers and said first cryptographic key producer for producing a second cryptographic key using the other of the first information and the second information, and said decipherer includes a first deciphering section and a second

deciphering section, said first deciphering section deciphering

the enciphered data using the first cryptographic key, and said

second deciphering section deciphering the data deciphered by

said first deciphering section using the second cryptographic

key.

63. The deciphering apparatus according to claim 62,

wherein said second deciphering section is formed from

application software for processing the deciphered data.

64. An enciphering method according to claim 46, wherein a

homomorphic cryptographic key is produced.

65. An enciphering method according to claim 46, wherein

said cryptographic key is produced with which a correct

decipherment result is obtained even if the first information and

the second information which compose the cryptographic key are

used individually to successively decipher the enciphered data.

66. An enciphering method according to claim 46, wherein

the second information is added to a value whose initial value is

the first information to produce the cryptographic key.

67. An enciphering method according to claim 66, wherein

the first information has a number of bits larger than that of

the second information, and the second information is added to

bits at predetermined positions of the first information, a bit

at a predetermined position of a result of the addition is

extracted and the extracted bit is further added to produce the

cryptographic key.